Installation Guide

# McAfee Threat Intelligence Exchange 1.0.0

For use with ePolicy Orchestrator 5.1.1 Software

## COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

## TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

## LICENSE INFORMATION

### License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents


**Preface** **5**

About this guide . . . . . 5

Audience . . . . . 5

Conventions . . . . . 5

Find product documentation . . . . . 6

**1 Installing Threat Intelligence Exchange** **7**

Requirements . . . . . 7

Install the Data Exchange Layer client . . . . . 8

Install Threat Intelligence Exchange server and module for VirusScan Enterprise . . . . . 9

Install the server appliance . . . . . 9

Create a new registered server . . . . . 17

Deploy the Data Exchange Layer client . . . . . 18

Deploy the Threat Intelligence Exchange module for VirusScan Enterprise . . . . . 18

Verify the installation . . . . . 18

Configure the server extension . . . . . 19

Configure the server policy . . . . . 19

Configure Data Exchange Layer brokers . . . . . 20

**2 Troubleshooting** **23**

Troubleshoot the installation . . . . . 23

Access the log files . . . . . 24

Reconfiguring using scripts . . . . . 24

**Index** **27**

# Preface

This guide provides the information you need to work with your McAfee product.

**Contents**


- *About this guide*
- *Find product documentation*


## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

### Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

### Conventions

This guide uses these typographical conventions and icons.

| | |
|---|---|
| *Book title*, *term*, *emphasis* | Title of a book, chapter, or topic; a new term; emphasis. |
| **Bold** | Text that is strongly emphasized. |
| `User input, code, message` | Commands and other text that the user types; a code sample; a displayed message. |
| **Interface text** | Words from the product interface like options, menus, buttons, and dialog boxes. |
| Hypertext blue | A link to a topic or to an external website. |
| | **Note:** Additional information, like an alternate method of accessing an option. |
| | **Tip:** Suggestions and recommendations. |
| | **Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data. |
| | **Warning:** Critical advice to prevent bodily harm when using a hardware product. |

# Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

## Task

1 Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.

2 Enter a product name, select a version, then click **Search** to display a list of documents.

# 1 Installing Threat Intelligence Exchange

McAfee® Threat Intelligence Exchange has several components. It has a module for McAfee® VirusScan® Enterprise, a server, and brokers that communicate with the Data Exchange Layer.

Install each Threat Intelligence Exchange component in the order presented here. When you are finished, these items are added to your network:

- Three McAfee® ePolicy Orchestrator® (McAfee ePO™) managed extensions:
  - Data Exchange Layer extensions
  - Threat Intelligence Exchange server extension
  - Threat Intelligence Exchange module for VirusScan Enterprise extension
- Threat Intelligence Exchange server/Data Exchange Layer server
- Threat Intelligence Exchange for VirusScan Enterprise module on each managed system in your network
- Data Exchange Layer client on each managed system in your network

**Contents**


- *Requirements*
- *Install the Data Exchange Layer client*
- *Install Threat Intelligence Exchange server and module for VirusScan Enterprise*
- *Deploy the Data Exchange Layer client*
- *Deploy the Threat Intelligence Exchange module for VirusScan Enterprise*
- *Verify the installation*
- *Configure the server extension*
- *Configure Data Exchange Layer brokers*


## Requirements

To make sure that your installation is successful, review these requirements before installing the Threat Intelligence Exchange software.

- Threat Intelligence Exchange software. You can access it from the Software Manager in McAfee ePO, or download it from the McAfee product download website.
  - Threat Intelligence Exchange server
  - Data Exchange Layer client
  - Threat Intelligence Exchange module for VirusScan Enterprise

- McAfee ePO 5.1.1 with the following managed product extensions and packages checked in:
  - VirusScan Enterprise 8.8 Patch 4 and Hotfix 929019
  - McAfee® Agent 5.0
  - McAfee Agent 5.0 extension
- VMware vSphere 5.1.0 with ESXi 5.1 and later
- The following products on your managed systems:
  - VirusScan Enterprise 8.8 Patch 4 and Hotfix 929019
  - McAfee Agent 5.0

### Operating system requirements

You can install Threat Intelligence Exchange on the following operating systems.

**Data Exchange Layer client**

| | |
|---|---|
| Microsoft Windows | Windows 7 (32-bit and 64-bit)<br>Windows 8.0 (32-bit and 64-bit)<br>Windows 8.1 (32-bit and 64-bit)<br>Windows 8.1U1/U2 (32-bit and 64-bit)<br>Windows Server 2008 R2<br>Windows Server 2012<br>Windows Server 2012 R2 |
| Non-Microsoft Windows | McAfee Linux OS (MLOS)<br>Other Linux operating systems<br>(for example, Red Hat, CentOS) |

**Threat Intelligence Exchange module for VirusScan Enterprise**

| | |
|---|---|
| Microsoft Windows | Windows 7 (32-bit and 64-bit)<br>Windows 8.0 (32-bit and 64-bit)<br>Windows 8.1 (32-bit and 64-bit)<br>Windows 8.1U1/U2 (32-bit and 64-bit)<br>Windows Server 2008 R2<br>Windows Server 2012<br>Windows Server 2012 R2 |

# Install the Data Exchange Layer client

Install the Data Exchange Layer software into McAfee ePO. It includes the client and broker software.

For details about installing software using McAfee ePO, see the *McAfee ePolicy Orchestrator Installation Guide*.

### Task

For option definitions, click **?** in the interface.

- Use one of these methods:
  - In the **Software Manager**, click **McAfee Data Exchange Layer 1.0**, then download or check in the components.
  - To install manually, download the McAfee Data Exchange Layer 1.0 files from the McAfee product download website. Then check in the Data Exchange Layer package to McAfee ePO.

# Install Threat Intelligence Exchange server and module for VirusScan Enterprise

Install the Threat Intelligence Exchange server and the module for VirusScan Enterprise.

### Task

For option definitions, click **?** in the interface.

- Use one of these methods:
  - In the **Software Manager**, click **McAfee Threat Intelligence Exchange 1.0**, then download or check in the components.
  - To install manually, download the McAfee Threat Intelligence Exchange 1.0 files from the McAfee product download website.

The Server Appliance is installed using VMware vSphere. Download the Server Appliance file and save it locally before continuing. The following tasks include detailed instructions for installing the server.

### Tasks

- *Install the server appliance* on page 9
  Install and configure the Threat Intelligence Exchange server and the Data Exchange Layer brokers.
- *Create a new registered server* on page 17
  To view Threat Intelligence Exchange information in McAfee ePO reports and dashboards, create a new registered server.

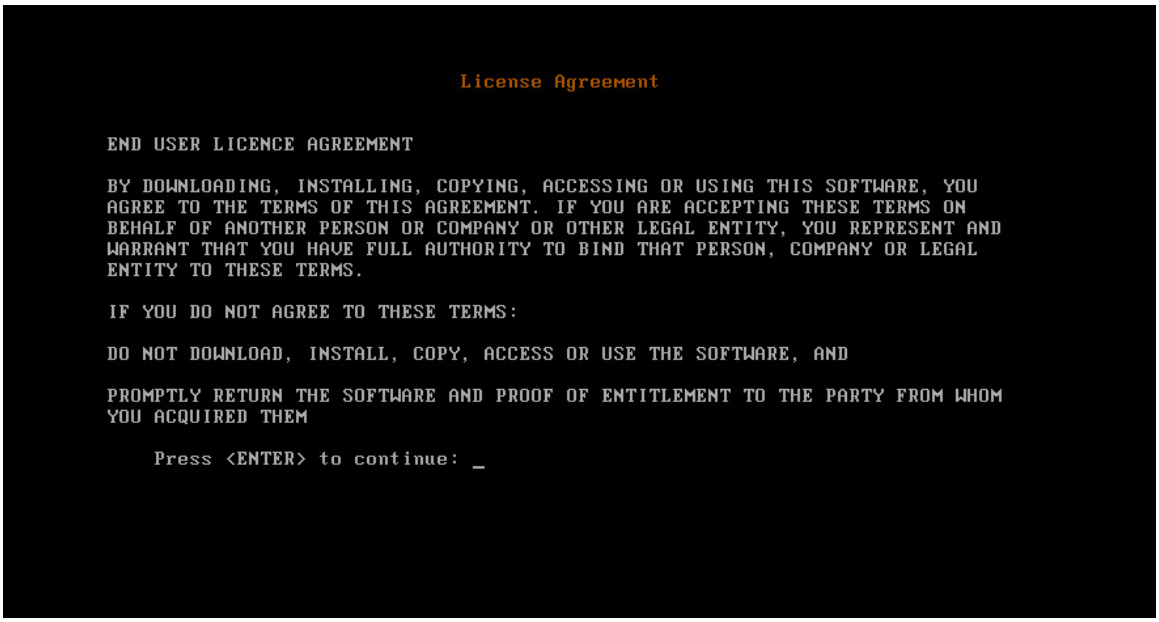
## Install the server appliance

Install and configure the Threat Intelligence Exchange server and the Data Exchange Layer brokers.

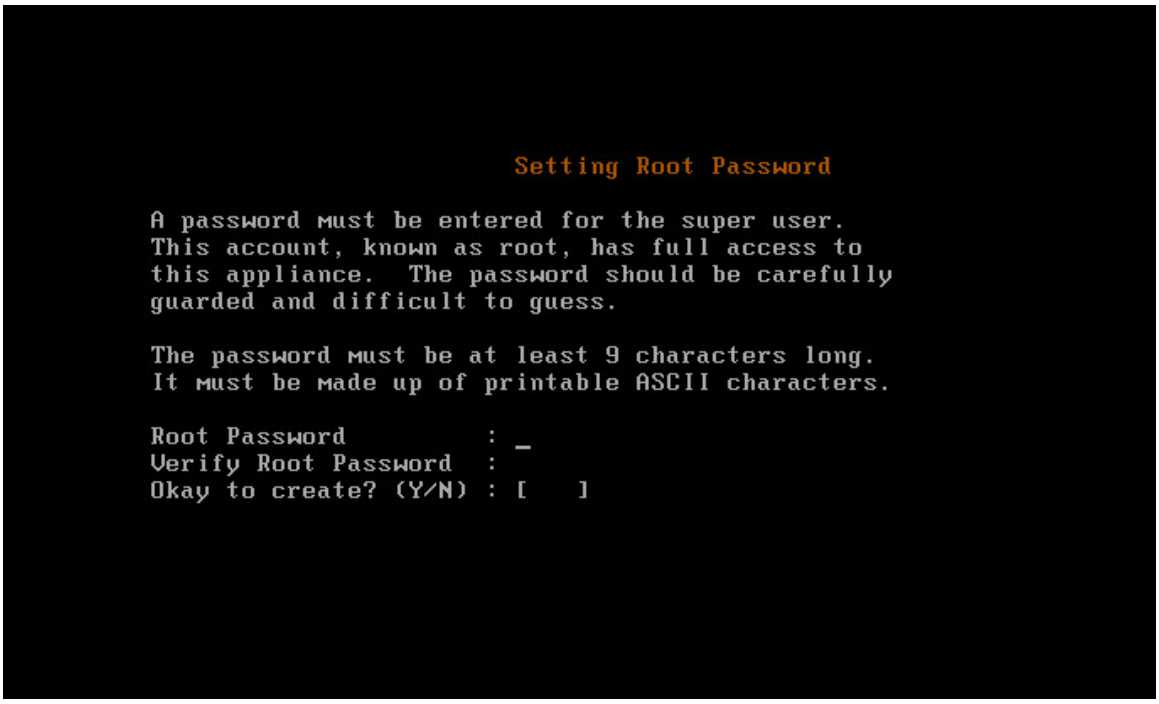
### Task

1. Open the VMware vSphere client and click **File** | **Deploy OVF Template**.
2. Browse to and select the .ova file on your computer, then click **Next**.
3. Complete the steps in the wizard, accepting the default values or entering different values as needed.
4. When finished, select **Power On** to turn on the virtual machine and open a **Console** window to install the server appliance.

5 Read and accept the license agreement. Press **Enter** several times to view each of the pages.

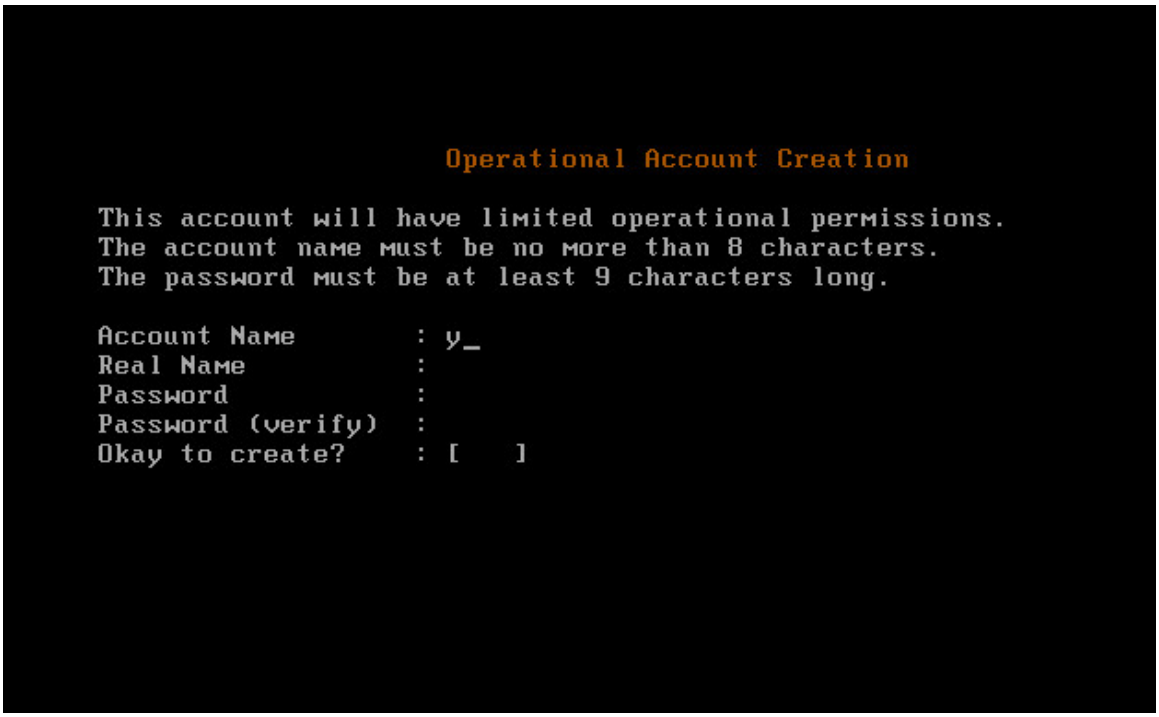

License Agreement
END USER LICENCE AGREEMENT
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING OR USING THIS SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY OR LEGAL ENTITY TO THESE TERMS.
IF YOU DO NOT AGREE TO THESE TERMS:
DO NOT DOWNLOAD, INSTALL, COPY, ACCESS OR USE THE SOFTWARE, AND
PROMPTLY RETURN THE SOFTWARE AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED THEM
Press <ENTER> to continue: _

6 Create a root password for the Threat Intelligence Exchange appliance. The password must be at least nine characters.

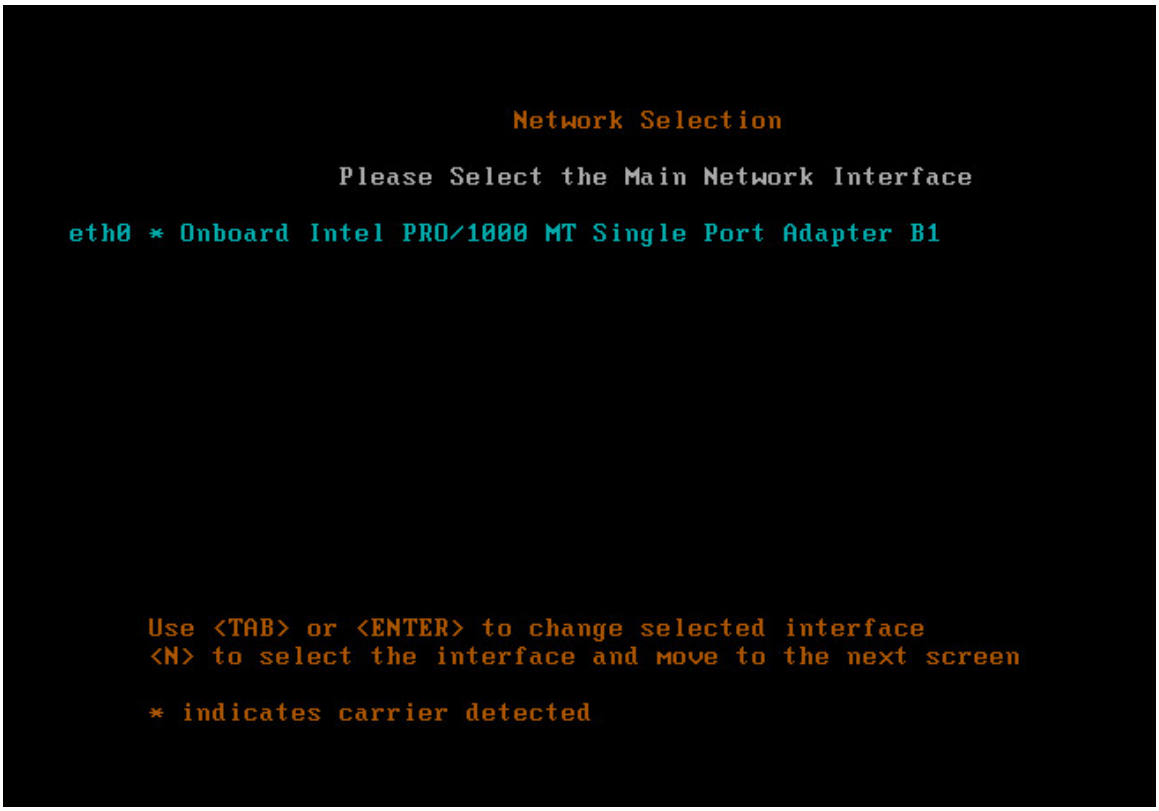

Setting Root Password
A password must be entered for the super user.
This account, known as root, has full access to
this appliance. The password should be carefully
guarded and difficult to guess.
The password must be at least 9 characters long.
It must be made up of printable ASCII characters.
Root Password : _
Verify Root Password :
Okay to create? (Y/N) : [ ]

7 Enter the operational account name, real name, and password, using the **Tab** key to move to each next field. When finished, press **Y** to continue.

This account has fewer permissions than the root account. The account name is typically something like `jsmith` and is used to log on to the server. The real name is your full name, for example, `John Smith`.

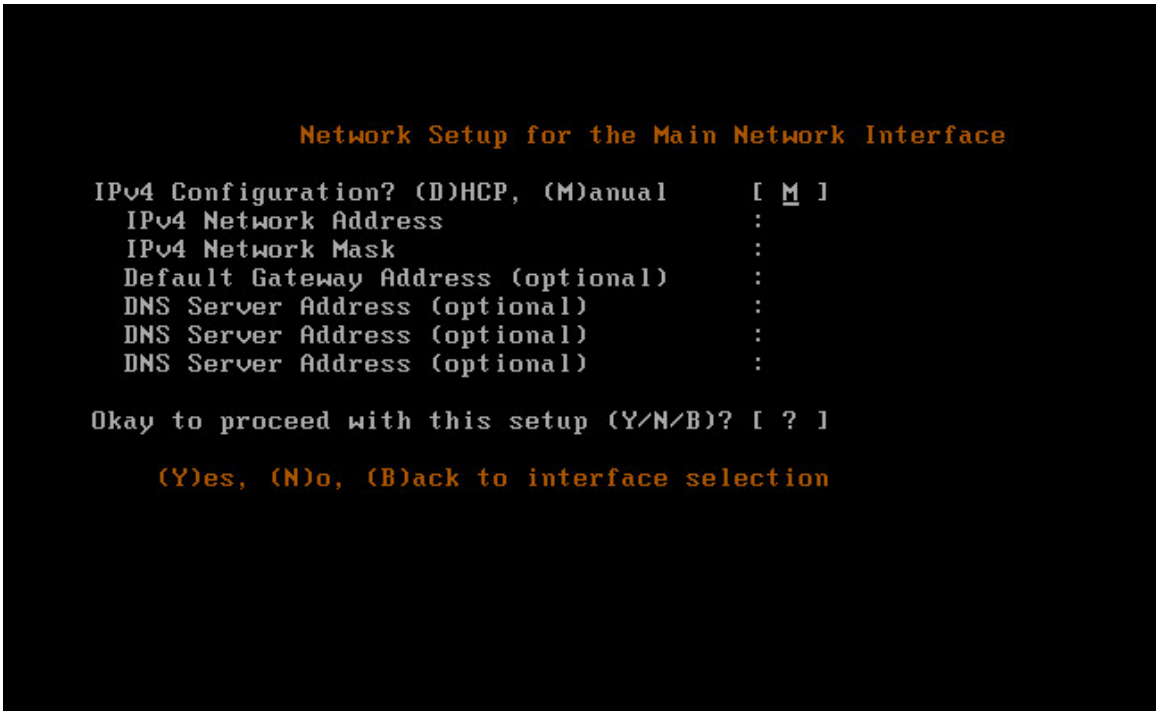

Operational Account Creation
This account will have limited operational permissions.
The account name must be no more than 8 characters.
The password must be at least 9 characters long.
Account Name : y_
Real Name :
Password :
Password (verify) :
Okay to create? : [ ]

8 One option appears on the Network Selection page; enter **N** to continue.


Network Selection
Please Select the Main Network Interface
eth0 * Onboard Intel PRO/1000 MT Single Port Adapter B1
Use <TAB> or <ENTER> to change selected interface
<N> to select the interface and move to the next screen
* indicates carrier detected

9 Select a configuration type, then enter **Y** to continue.

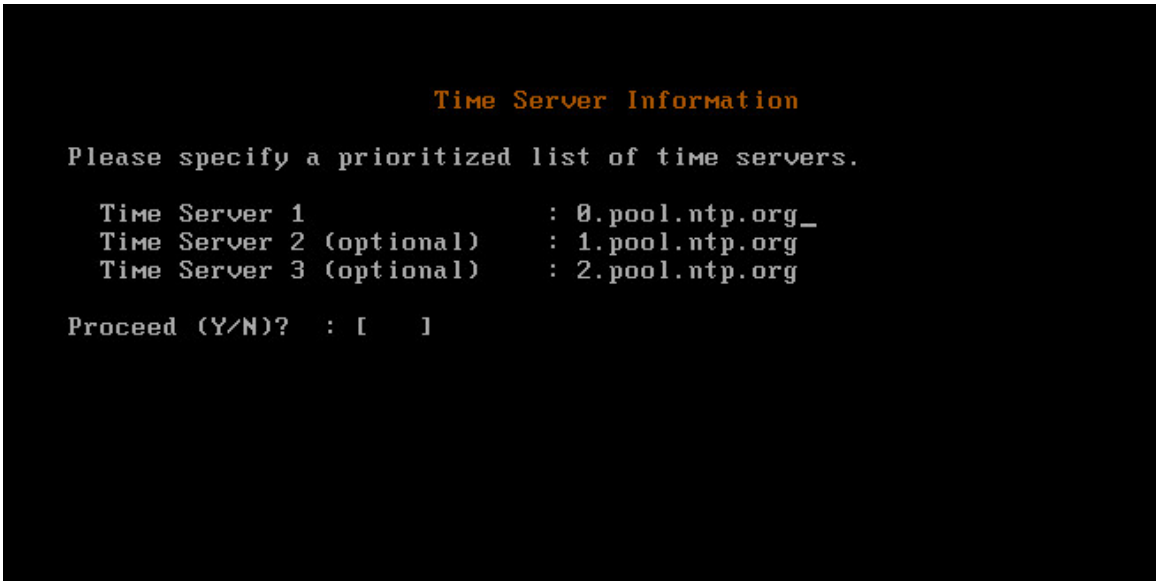
- DHCP — Enter **D**.
- Manual IP address — Enter **M**, then enter the remaining information.


Network Setup for the Main Network Interface
IPv4 Configuration? (D)HCP, (M)anual [ M ]
IPv4 Network Address :
IPv4 Network Mask :
Default Gateway Address (optional) :
DNS Server Address (optional) :
DNS Server Address (optional) :
DNS Server Address (optional) :
Okay to proceed with this setup (Y/N/B)? [ ? ]
(Y)es, (N)o, (B)ack to interface selection

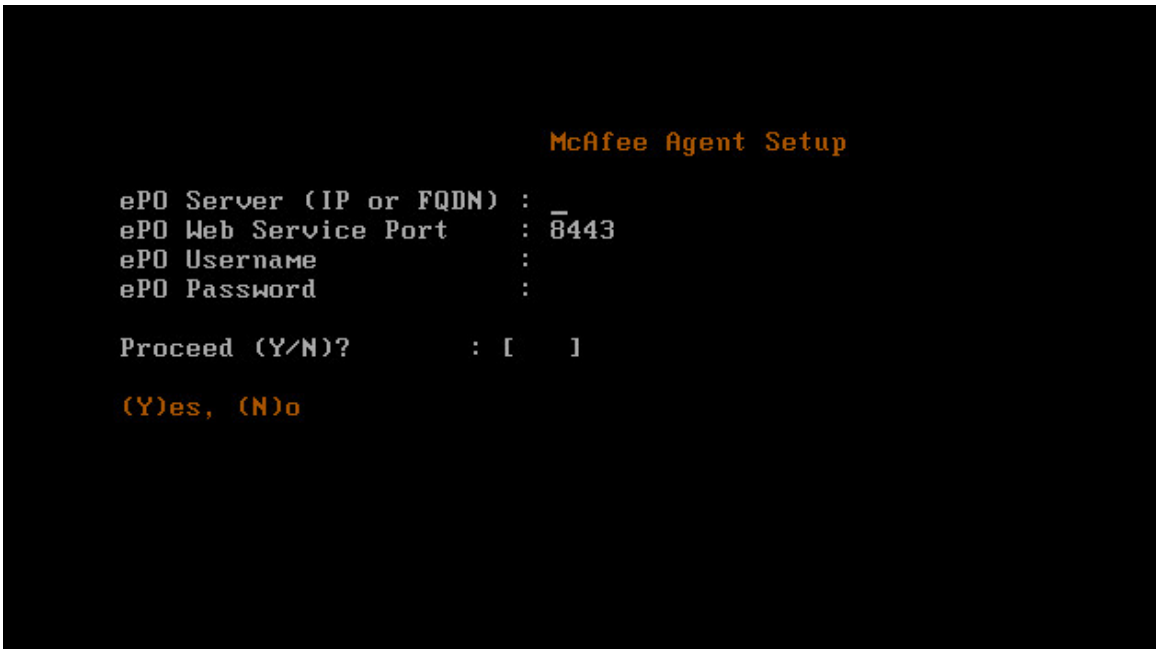
10 Enter the fully qualified host name and domain name of the computer where you are installing the Threat Intelligence Exchange server appliance. Enter **Y** to continue.

Please enter a Hostname for this system. Valid characters are [a-z][0-9]-
Enter a domain name also, if appropriate.
Hostname : _
Domain Name :
Okay to create? (Y/N)? : [ ]

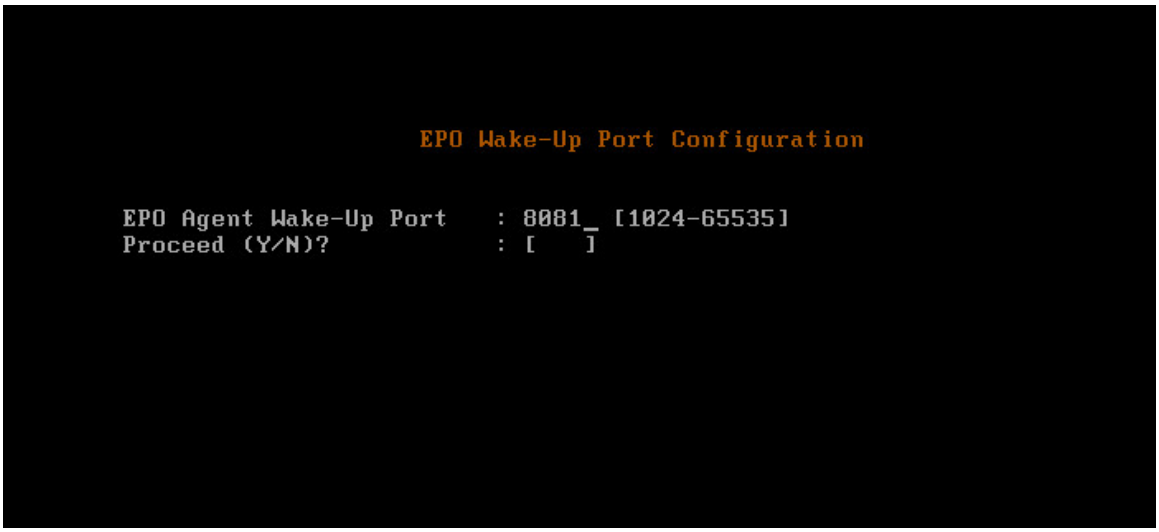
11 Enter up to three Network Time Protocol servers to synchronize the time of the Threat Intelligence Exchange server. Use the default servers listed, or enter the address for up to three servers. Enter **Y** to continue.


Time Server Information
Please specify a prioritized list of time servers.
Time Server 1 : 0.pool.ntp.org_
Time Server 2 (optional) : 1.pool.ntp.org
Time Server 3 (optional) : 2.pool.ntp.org
Proceed (Y/N)? : [ ]

12 Enter the IP address or fully qualified domain name, port, and account information for your McAfee ePO server. The user account must have administrator rights. Enter **Y** to continue.

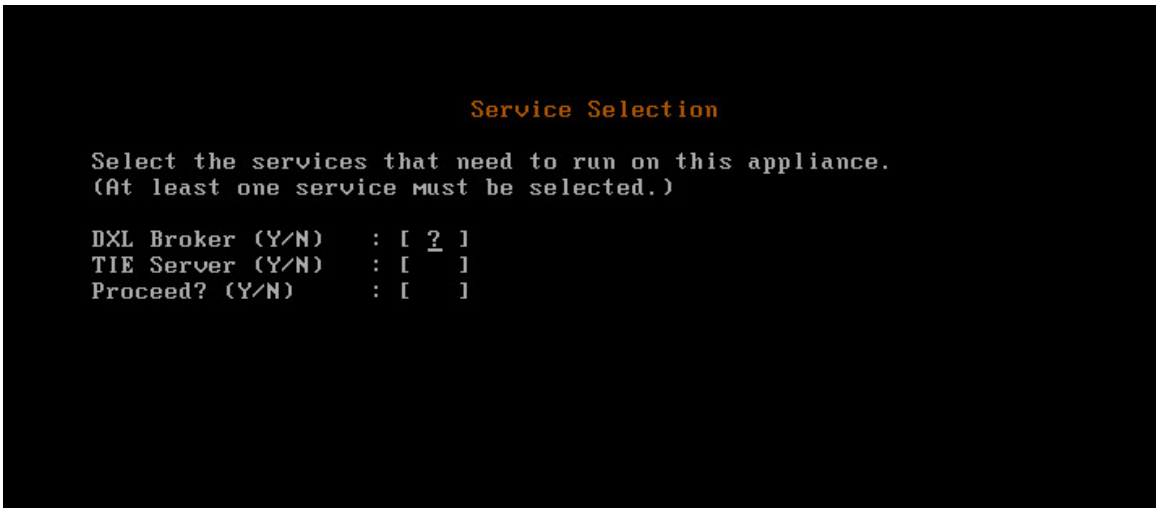



13 To receive wake-up requests from McAfee ePO, verify the port used by the McAfee Agent on the Threat Intelligence Exchange server. Enter **Y** to continue.

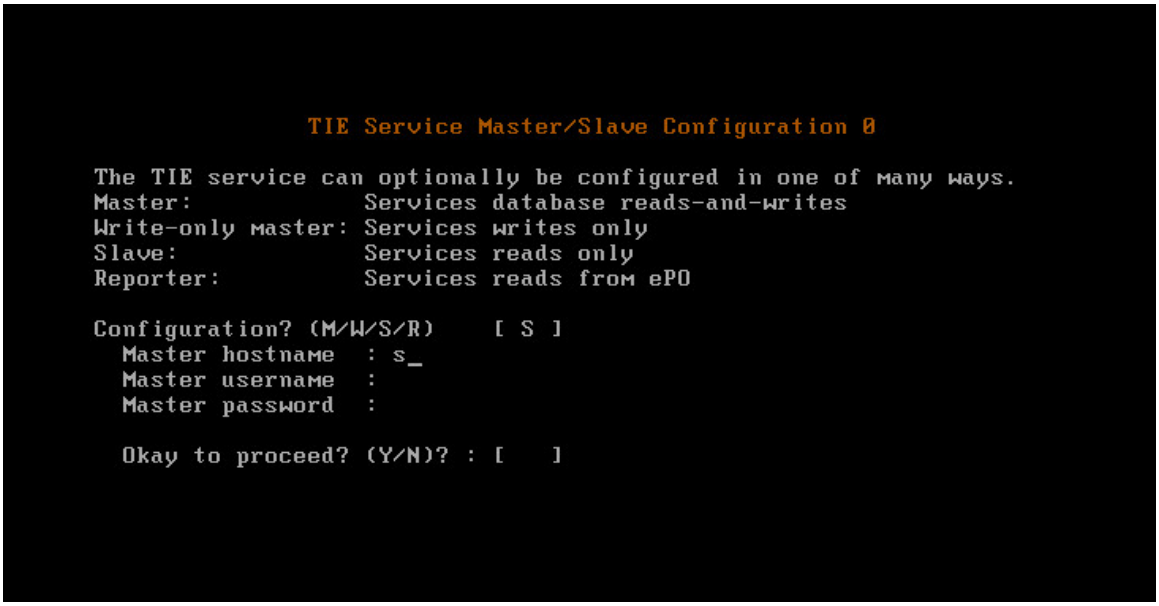



14 Select the services to run on the Threat Intelligence Exchange server, then enter **Y** to continue.

Run this installation multiple times to set up the brokers and servers where you want them. You can install brokers on some systems, a server on a different system, or a broker and server on the same system. You must install at least one broker.


Service Selection
Select the services that need to run on this appliance.
(At least one service must be selected.)
DXL Broker (Y/N) : [ ? ]
TIE Server (Y/N) : [ ]
Proceed? (Y/N) : [ ]

The following page, which appears only if you selected the **TIE Server** option on the previous page, specifies how to configure the Master and Slave servers. You can have only one Master server in your environment, but you can have several optional Slave servers.


TIE Service Master/Slave Configuration 0
The TIE service can optionally be configured in one of many ways.
Master: Services database reads-and-writes
Write-only master: Services writes only
Slave: Services reads only
Reporter: Services reads from ePO
Configuration? (M/W/S/R) [ S ]
Master hostname : s
Master username :
Master password :
Okay to proceed? (Y/N)? : [ ]

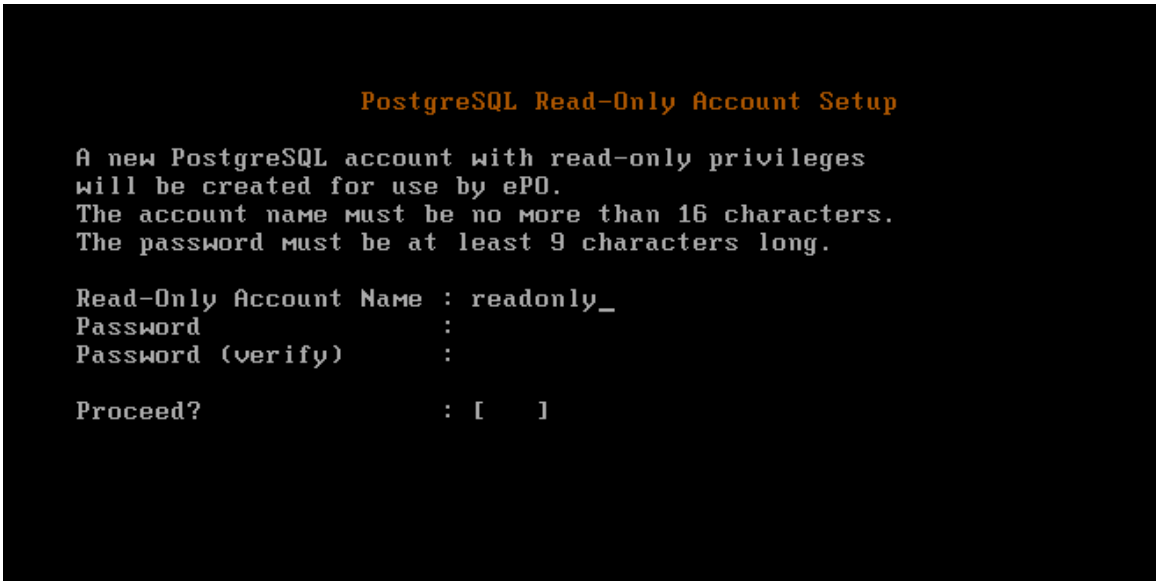
If you are installing more than one server, install the Master server first, then install the Slave servers on other systems in your environment. You enter the Master server information on those systems when installing Slave servers.

- **Master** server replicates the Threat Intelligence Exchange database to all Slave servers, if you have them.
- **Write-only Master** server doesn't process reputation requests or any non-essential functionality beyond writing and maintaining the database. Because a write-only Master server doesn't process requests over the Data Exchange Layer, it increases system performance by replicating the database, leaving the Data Exchange Layer requests to the Slave servers.

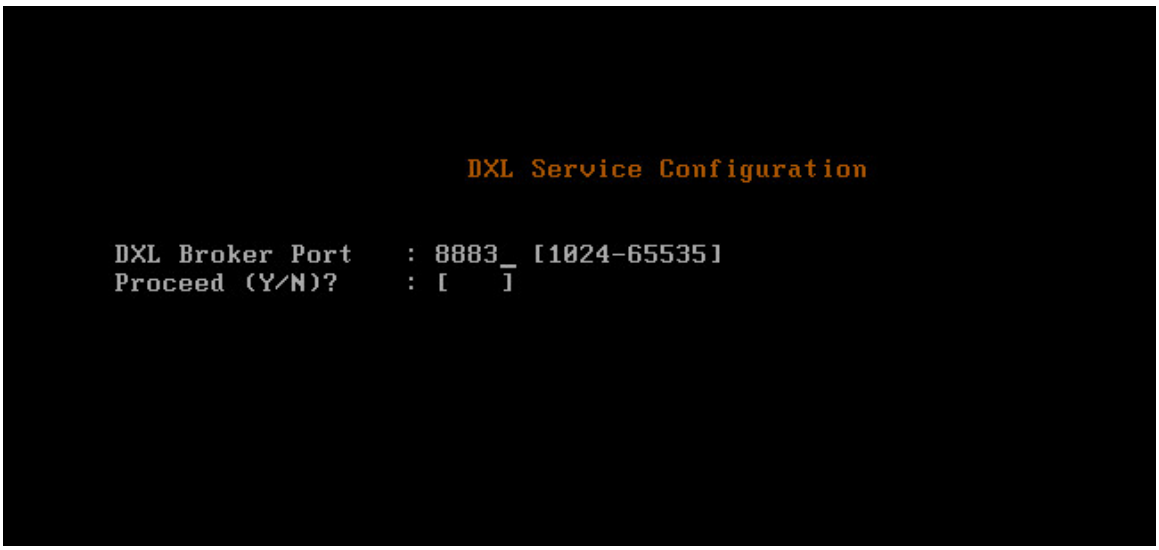
- **Slave** server processes Data Exchange Layer requests exactly like a Master server, using a database that's replicated from the Master database. The Slave server must have access to the Master server.
- **Reporter** is a Slave server that does not process reputation requests. It improves McAfee ePO reporting by replicating the database information without processing Data Exchange Layer requests.

15 The PostgreSQL account enables the Threat Intelligence Exchange server to communicate with McAfee ePO. You enter this account information in the McAfee ePO **Registered Servers** option in a later step to allow McAfee ePO to connect to and receive data from the Threat Intelligence Exchange server.

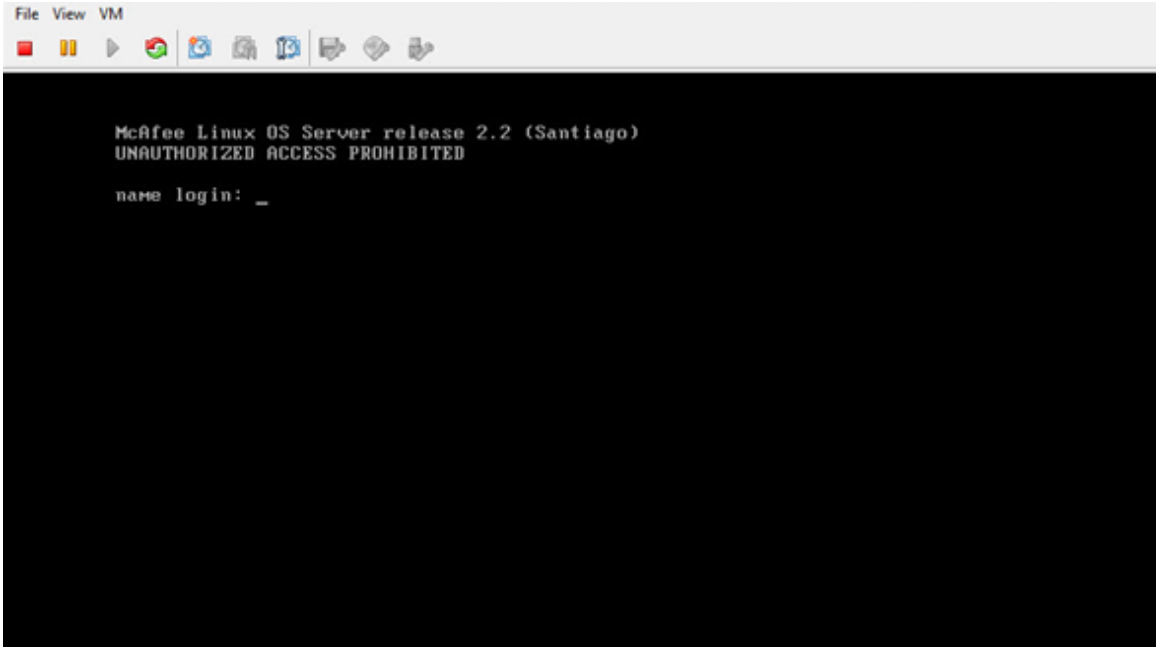
The account name and password can be anything you like within the stated parameters.


PostgreSQL Read-Only Account Setup
A new PostgreSQL account with read-only privileges
will be created for use by ePO.
The account name must be no more than 16 characters.
The password must be at least 9 characters long.
Read-Only Account Name : readonly_
Password :
Password (verify) :
Proceed? : [ ]

16 Specify the port that the Data Exchange Layer uses. Use the default port, or enter a port number within the range shown, then enter **Y** to continue.



17 Do nothing on this page and close it.




18 Verify that the Threat Intelligence Exchange server is provisioned: open the **System Tree** in McAfee ePO and look in the domain where you installed the server appliance.

If provisioned correctly, the server is listed as a managed system.

## Create a new registered server

To view Threat Intelligence Exchange information in McAfee ePO reports and dashboards, create a new registered server.

### Task

For option definitions, click **?** in the interface.

1 In McAfee ePO, click **Menu** | **Configuration** | **Registered Servers**, then click **New Server**.

2 In the **Server type** drop-down list, click **Database Server**.

3 Enter a **Name**, for example, `TIE Server`, then click **Next**.

4 On the **Details** page:

a Select the checkbox for **Make this the default database for the selected database type**.

This option is automatically selected when you create the first registered server. If you have more than one Threat Intelligence Exchange database, select this option only for the database you want as the default.

b In the **Database Vendor** field, select **TieServerPostgres**.

c In the **Host name or IP address** field, enter the IP address of the system where you installed the server.

d Leave the **Database server instance** and **Database server port** fields blank (if they appear).

e For the **Database name**, enter `tie`.

f In the **User name** and **password** fields, enter the read-only postgress user name and password that you specified on the PosgresSQL page during the server installation.

5 Click **Test Connection**.

McAfee ePO communicates with the server and retrieves data for the reports and dashboards.

# Deploy the Data Exchange Layer client

Deploy the Data Exchange Layer client to each of your managed systems.

### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Software** | **Product Deployment**, then click **New Deployment**.

2 Complete the new deployment information, then start the deployment.

For details about deploying software in McAfee ePO, see the *McAfee ePolicy Orchestrator Product Guide*.

# Deploy the Threat Intelligence Exchange module for VirusScan Enterprise

Deploy the module for VirusScan Enterprise to each of your managed systems. The Threat Intelligence Exchange policies assigned to those systems block and prompt based on the policy settings.

> **Before you begin**
>
> Each system must be running McAfee Agent 5.0, VirusScan Enterprise, Patch 4 with Hotfix 929019, and the Data Exchange Layer client.

### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Software** | **Product Deployment**, then click **New Deployment**.

2 Complete the new deployment information, then start the deployment.

For details about deploying software in McAfee ePO, see the *McAfee ePolicy Orchestrator Product Guide*.

# Verify the installation

After installing the Threat Intelligence Exchange and Data Exchange Layer components, perform these tasks to verify the installation.

### Task

For option definitions, click **?** in the interface.

1 In the **System Tree**, click the Threat Intelligence Exchange server name, then click the **Products** tab. Verify that the following components are listed:
   - McAfee DXL Broker
   - McAfee DXL Client
   - McAfee Threat Intelligence Exchange Server

2 In the **System Tree**, verify that the TIESERVER tag was applied to the system.

3 Click **Menu** | **Configuration** | **Server Settings**, then click **DXL ePO Client**.

   Verify that the **Connection State** is **Connected**.

4 In the **System Tree**, select the Threat Intelligence Exchange server, then from the **Actions** menu, click **DXL** | **Lookup in DXL**.

5 Verify that the **Connection State** is **Connected**.

The DXL broker is now up and running. You can click **Menu** | **Systems Section** | **TIE Reputations** to verify that you can search for files and certificates. It might take some time for reputation information to populate the database. If you can't search for files and certificates, see *Troubleshooting*.

# Configure the server extension

If you use VirusTotal, enter your public or private key to access additional file reputation information.

VirusTotal is a free service that analyzes files and helps to detect viruses, trojans, and other malware. You can access VirusTotal data directly from Threat Intelligence Exchange when viewing file reputation information.

### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Server Settings** | **Threat Intelligence Exchange Server**.

2 Click **Edit** and enter your VirusTotal key.

When viewing file reputations on the **TIE Reputations** page, click the **VirusTotal** tab to see additional file information.

### Tasks

- *Configure the server policy* on page 19
  Specify McAfee GTI and McAfee Advanced Threat Defense settings for the server.

# Configure the server policy

Specify McAfee GTI and McAfee Advanced Threat Defense settings for the server.

### Task

For option definitions, click **?** in the interface.

1 In McAfee ePO, click **Menu** | **Policy** | **Policy Catalog**.

2 From the **Product** drop-down list, click **McAfee Threat Intelligence Exchange Server Management 1.0.0**, then select a policy name or an action.

You can create a policy using **Default** as a template, or copy an existing policy and change it as needed.

3 On the **General** tab:

- **GTI Reputations** — Specify whether to use McAfee GTI to get file reputation. McAfee GTI is used if the Threat Intelligence Exchange server does not have reputation information for a file, or if the server is unavailable (offline).
- **Proxy Settings for GTI Requests** — If you use a web proxy for Internet access and it requires authentication, enter the proxy information.
- **Product Improvement Program** — Specify whether to send file and certificate information to McAfee. For details about what is sent to the McAfee Product Improvement Program, see the *Threat Intelligence Exchange Product Guide.*

4 On the **Advanced Threat Defense** tab, specify whether to send file information to Advanced Threat Defense for further evaluation. Enter the Advanced Threat Defense server name and access credentials, available servers, and timeout settings.

For details about how Advanced Threat Defense works with Threat Intelligence Exchange, see the *Threat Intelligence Exchange Product Guide*.

# Configure Data Exchange Layer brokers

If you installed Data Exchange Layer brokers on more than one system, you can create a hierarchy of brokers to provide failover protection if any brokers are unavailable.

Brokers can be organized into hubs and service zones that contain one or two brokers.

**Brokers** — Installed on managed systems and communicate messages between Threat Intelligence Exchange modules. The network of brokers tracks active clients and dynamically adjusts the message routing as needed. Brokers can be organized into hubs.

**Hubs** — Contain one or two brokers that are associated with a specific location. Hubs manage the way brokers are accessed and provide failover protection in a multi-broker environment. If a hub has two brokers, both act simultaneously. If one is unavailable, the other continues to function. You can create as many hubs as needed. A broker, however, can be assigned to only one hub.

**Service zones** — A service zone is associated with a broker or hub and determines the way brokers are accessed. For example, if you have multiple Threat Intelligence Exchange servers and brokers in different geographical locations, you can create service zones of servers and brokers so that local clients access brokers in their area. Clients in a service zone access brokers in that zone first. If those brokers are not available, the clients access the brokers in other zones.

## Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Configuration** | **Server Settings** | **DXL Topology**.
2. On the DXL Topology page, select **Edit** to create hubs, service zones, and assign brokers.

   Brokers not assigned to a hub are listed below the hubs.
3. Select an item from the **Actions** menu to create or delete a hub, or to detach a broker from its current hub.

# 2 Troubleshooting

Find solutions for common issues that might occur during installation. You can also access scripts for reconfiguring the Threat Intelligence Exchange server, Data Exchange Layer brokers, and the McAfee Agent.

**Contents**


- *Troubleshoot the installation*
- *Access the log files*
- *Reconfiguring using scripts*


## Troubleshoot the installation

If you experience problems installing and accessing the Threat Intelligence Exchange module for VirusScan Enterprise, server, or the Data Exchange Layer client, follow these steps.

**Task**

For option definitions, click **?** in the interface.

1. In McAfee ePO, click **Menu** | **System Tree**, then select the checkbox for the Threat Intelligence Exchange server.
2. Click **Wake Up Agents**.
3. On the **Wake Up McAfee Agent** page, select **Force complete policy and task update**, then click **OK**.

   This option sends the server properties from the Threat Intelligence Exchange appliance to McAfee ePO. Verify that this task completed in the server task log.
4. In the **System Tree**, click the server name, then click the **Products** tab. Verify that these components are listed:
   - McAfee DXL Broker
   - McAfee DXL Client
   - McAfee Threat Intelligence Exchange Server
5. Click **Menu** | **Automation** | **Server Tasks** and run the task: **Apply TIESERVER tags to TIE Server**.

   In the **System Tree**, verify that the TIESERVER tag was applied to the system. Verify that this task completed in the server task log.
6. Click **Menu** | **Automation** | **Server Tasks** and run the task: **Manage DXL Brokers**.

   In the **System Tree**, verify that the DXLBROKER tag was applied to the system. Verify that this task completed in the server task log.

7 After the tags are successfully applied, click **System Tree**, select the Threat Intelligence Exchange server, then click **Wake Up Agents**.

8 On the **Wake Up McAfee Agent** page, select **Force complete policy and task update**, then click **OK**.

Verify that this task completed in the server task log.

9 Click **Menu** | **Configuration** | **Server Settings**, then click **DXL ePO Client**.

a Verify that the **Connection State** is **Connected**. If it isn't, repeat steps 5–8.

b Verify that the DXL and TIE services are running: on the virtual machine, open a Console window, log on and enter `service dxlbroker status`, then enter `service tieserver status`.

10 In the **System Tree**, select the Threat Intelligence Exchange server, and from the **Actions** menu, click **DXL** | **Lookup in DXL**.

a Verify that the **Connection State** is **Connected**.

b Verify that the DXL and TIE services are running: on the virtual machine, open a Console window, log on and enter `service dxlbroker status`, then enter `service tieserver status`.

With the DXL broker up and running successfully, you can now click **Menu** | **Systems Section** | **TIE Reputations** to verify that you can search for files and certificates. If you can't, repeat steps 5–8.

# Access the log files

To troubleshoot installation problems, see the following log files.

**Threat Intelligence Exchange server** — `/var/McAfee/tieserver/logs/tieserver.log`

**Threat Intelligence Exchange module for VirusScan Enterprise** — `%programdata%\McAfee\TIEM`

**Data Exchange Layer Client** — `%programdata%\McAfee\Data_eXchange_Layer`

**Data Exchange Layer Broker** — `/var/McAfee/dxlbroker/logs/dxlbroker.log`

# Reconfiguring using scripts

Scripts are available to reconfigure the Threat Intelligence Exchange server, Data Exchange Layer brokers, and the McAfee Agent.

## Accessing the scripts

The scripts are located in the `/home/<username>` directory. They must be executed with sudo permissions, for example, `sudo /home/myname/change-hostname`.

| Script name | Description |
|---|---|
| **change-hostname** | Changes the host name of the current server appliance. It restarts the McAfee Agent, the Threat Intelligence Exchange server, and the Data Exchange Layer broker.<br>A reboot is not needed but is recommended. |
| **change-services** | Enables or disables the Threat Intelligence Exchange server and Data Exchange Layer broker.<br>If the server was initially disabled during first boot, the script prompts for server configuration information. If the broker was initially disabled, the script prompts for broker configuration information.<br>A reboot is not needed. |
| **reconfig-dxl** | Reconfigures the Data Exchange Layer port.<br>A reboot is not needed. |
| **reconfig-ma** | Reconfigures the McAfee Agent.<br>The agent, Threat Intelligence Exchange server, and Data Exchange Layer broker services are restarted. New keystores are generated when the service starts.<br>A reboot is not needed but is recommended. |
| **reconfig-network** | Reconfigures the current network interface (from DHCP to manual, or from manual to DHCP).<br>A server reboot is **required**. |
| **reconfig-ntp** | Reconfigures the Network Time Protocol servers.<br>A reboot is not needed. |
| **reconfig-tie** | Changes the role of the Threat Intelligence Exchange server. For example, change the server from a Slave to a Master, or from a Master to a Reporter.<br>A reboot is not needed. |

# Index


## A

about this guide 5
Advanced Threat Defense settings 19

## B

broker configuration 20

## C

configuration
    Data Exchange Layer brokers 20
    scripts, reconfiguring the server 24
    server policy settings 19
    VirusTotal, file reputation information 19
conventions and icons used in this guide 5

## D

Data Exchange Layer
    configuring brokers 20
    deploying 18
    hubs 20
    installation requirements 7
    installing 8
    reconfiguring using scripts 24
    supported operating systems 7
    topology 20
    troubleshooting the installation 23
    verifying the installation 18
deployment
    Data Exchange Layer client 18
    module for VirusScan Enterprise 18
    OVF template 9
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5

## F

failover protection, organizing brokers 20

## G

Global Threat Intelligence server settings 19

## H

hubs
    creating 20
    organizing brokers 20

## I

installation
    components 7
    Data Exchange Layer 8
    log files for troubleshooting 24
    overview 7
    requirements 7
    server appliance 9
    Threat Intelligence Exchange server 9
    troubleshooting 23
    verifying the installation 18

## L

log files, troubleshooting the installation 24

## M

McAfee Agent
    installation requirements 7
    reconfiguring using scripts 24
McAfee ePO registered server, creating 17
McAfee ServicePortal, accessing 6
module for VirusScan Enterprise
    deploying 18
    installation requirements 7
    installing 9
    supported operating systems 7
    troubleshooting the installation 23
    verifying the installation 18

## O

operating systems, supported 7

## P

policy settings 19
Product Improvement Program settings 19

## R

reconfiguration using scripts 24
registered server, creating 17
reports, creating a registered server 17
requirements for installation 7

## S

scripts for reconfiguring 24
server appliance, installing 9
server policy settings 19
service zones, organizing brokers 20
ServicePortal, finding product documentation 6
settings, configuring the server policy 19
supported operating systems 7

## T

technical support, finding product information 6
Threat Intelligence Exchange
    installing 7
    troubleshooting the installation 23
Threat Intelligence Exchange server
    Advanced Threat Defense settings 19
Threat Intelligence Exchange server *(continued)*
    configuring 19
    Global Threat Intelligence settings 19
    installing 9
    policy settings 19
    Product Improvement Program settings 19
    reconfiguring using scripts 24
    server appliance 9
    troubleshooting the installation 23
troubleshooting
    installation issues 23
    viewing log files for installation issues 24

## V

verification, installation success 18
VirusTotal, accessing file reputation information 19
VMware vSphere
    deploying the OVF template 9
    installation requirements 7

McAfee
An Intel Company